Title (en)

ANONYMOUS AUTHENTICATION SIGNATURE SYSTEM, USER DEVICE, VERIFICATION DEVICE, SIGNATURE METHOD, VERIFICATION METHOD, AND PROGRAM THEREFOR

Title (de)

ANONYMES AUTHENTIFIKATIONSSIGNATURSYSTEM, BENUTZERVORRICHTUNG, VERIFIZIERUNGSVORRICHTUNG, SIGNATURVERFAHREN, VERIFIZIERUNGSVERFAHREN UND PROGRAMM DAFÜR

Title (fr)

SYSTÈME DE SIGNATURE D'AUTHENTIFICATION ANONYME, DISPOSITIF UTILISATEUR, DISPOSITIF DE VÉRIFICATION, PROCÉDÉ DE SIGNATURE, PROCÉDÉ DE VÉRIFICATION ET PROGRAMME CORRESPONDANT

Publication

EP 2456119 A4 20150408 (EN)

Application

EP 10799756 A 20100706

Priority

- JP 2010061449 W 20100706
- JP 2009164884 A 20090713

Abstract (en)

[origin: EP2456119A1] The user device includes: a recording unit which stores system parameters as respective parameters given in advance, a Disclosure public key, a use public key, a user private key, a member certificate, and an attribute certificate; an input/output unit which receives input of the Document from the user and an attributes the user intends to disclose; a cryptograph generating module which generates a cryptograph based on the inputted document, the attributes to be disclosed, and each of the parameters; a signatures text generating module which generates a zero-knowledge signature text from the generated cryptograph; and a signature output module which outputs the cryptograph and the zero-knowledge signature text as the signature data. The user public key and the attribute certificate are generated by using a same power.

IPC 8 full level

H04L 9/32 (2006.01); **G09C 1/00** (2006.01)

CPC (source: EP US)

H04L 9/3218 (2013.01 - EP US); **H04L 9/3249** (2013.01 - EP US)

Citation (search report)

- [A] US 2008133917 A1 20080605 - JEONG IK RAE [KR], et al
- [AD] CAMENISCH J ET AL: "A signature Scheme with Efficient Protocols", LECTURE NOTES IN COMPUTER SCIENCE/COMPUTATIONAL SCIENCE > (EUROCRYPT)CHES 2008 (LNCS), SPRINGER VERLAG, DE, vol. 2576, 1 January 2003 (2003-01-01), pages 268 - 289, XP002456613, ISBN: 978-3-540-24128-7, DOI: 10.1007/3-540-36413-7_20
- [AL] CAMENISCH J ET AL: "Efficient Non-transferable Anonymous Multi-show Credential System with Optional Anonymity Revocation", 27 November 2000 (2000-11-27), pages 1 - 34, XP002616976, Retrieved from the Internet <URL:http://www.zurich.ibm.com/~jca/papers/rz3295.pdf> [retrieved on 20110117]
- See references of WO 2011007697A1

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR

DOCDB simple family (publication)

EP 2456119 A1 20120523; **EP 2456119 A4 20150408**; **EP 2456119 B1 20160928**; JP 5532048 B2 20140625; JP WO2011007697 A1 20121227; US 2012124379 A1 20120517; US 8949609 B2 20150203; WO 2011007697 A1 20110120

DOCDB simple family (application)

EP 10799756 A 20100706; JP 2010061449 W 20100706; JP 2011522786 A 20100706; US 201013383476 A 20100706